ECE 628 - Computer Network Security
Winter 2024

Instructor: Professor G. Gong
Office: E7 5436, x45650, ggong@uwaterloo.ca
https://uwaterloo.ca/scholar/ggong
Office hours: TBA

Course Description

This course focuses on the fundamental principles of computer network security. The topics to be covered include symmetric-key and public-key cryptography, zero-knowledge proofs, semantic security, network and wireless security, multicast security, trusted platform, temple response hardware, physical layer security, decentralized system security, blockchain and cryptocurrency, data privacy enhanced technologies, secure machine learning, post-quantum cryptography and quantum key distribution.

Background Requirements Students attending this course should have a good working knowledge of probability theory and computer networks.

Resources Lectures: 01:00-3:50Th, E5 5106

References There is no textbook for the course, but the following references will be helpful for your reading.

1. M.T. Goodrich and R. Tamassia, *Introduction to Computer Security*, Addison Wesley, 2011 (GT11) (Section 3.3, Chapters 6, Sections 9.1, 9.6-9.7).

2. L.D. Chen and G. Gong, *Communication System Security*, CRC, 2012 (CG12).

3. W. Stallings and L. Brown, Computer Security: Principles and Practice, 4th edition, Pearson, 2017 (Part Five: Chapters 22-24) (SB17).

4. J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd edition, Chapman and Hall/CRC, 2014 (you may read it if you wish to have a deep crypto knowledge for your future career, but not required from the course).

5. Supplemental materials for the book by Chen-Gong (SM4CG12).

6. ECE 628 Course Notes -Available on UW-LEARN.

7. Selected papers.

Course Outline I have included a list of topics to be covered in the class, the reading materials and a corresponding rough time schedule. The list may be changed and refined during the course depending on the pace of the class. Notes and some additional readings links will be provided when the lectures go on.

1. Introduce to Basics of Computer Network Security: confidentiality, integrity and authentication, active and passive attacks, basic security protection mechanisms.

2. Networks and Security Metrics: entry point attacks, secure infrastructure, trust and threat model, Shannon's secrecy, complexity theory, semantic security, and pseudorandom generators.

3. Symmetric-key Cryptographic Systems: Linear feedback shift register based pseudorandom generation, stream ciphers and block ciphers, encryption models, chosen plaintext/ciphertext attack (CPA), secure hash functions, MAC, authenticated encryption, correlation attacks and time-memory trade-off attacks.

4. Public-key Systems: security of public-key cryptography, basic schemes, digital signature, ECC, pairing-based IBC, fully homomorphic encryption, post-quantum digital signature, and fault attacks.

5. Network and Wireless Security: the man-in-the-middle attacks, mutual authentication and key establishment, cipher suite negotiation, network security protocols (IPsec, TLS/SSL, VPN), and attacks on TLS, radio air link protection (4G-LTE, 5G), IEEE 802.11 security solutions (flowed WEP, CCMP), jamming and relay attacks.

6. Broadcast and Multicast Security: multicast key distribution, hash chain, broadcast message authentication, Merkle tree based authentication and commitment.

7. Trusted Platform and System Security: trusted platform, temple response hardware, secure storage, remote attestation, anonymous authentication, and physical layer security.

8. Decentralized System Security: consensus, practical Byzantine fault tolerance, blockchain, Bitcoin and cryptocurrency, smart contract, zero knowledge proofs and Zcash, and applications to supply-chain management.

9. Privacy Enhanced Technologies: differential privacy, secret sharing, multiparty computation, and secure machine learning.

10. Post-quantum and Quantum Cryptography: one-time digital signature, quantum encryption, and quantum key distribution.

Topics	Suggested Reading Materials	Schedule
1. Introduction to Computer Network Security	1) Chapter 1 in CG12, 2) NIST, FIP-199*, 3) Diffie and Hellman, New Directions in Cryptography, 1976.	Week 1, Lecture 1
2. Networks and Security Metrics	Section 1.1 in GT11, Chapter 2 in SM2CG12.	Week 2, 1st half of Lecture 2
3. Symmetric-key Cryptographic Systems	Chapter 2-4 in CG12, and Chapter 3 in SM4CG12.	Week 2, 2nd half of Lecture 2, Week 3-Lecture 3
4. Public-key Systems	Chapter 5 in CG12, Chapter 4 in SM4CG12.	Week 4 - Lecture 4
5. Network and Wireless Security	Chapters 7-8 in CG12 or Chapter 22 in SB17	Week 5 - Lecture 5
6. Broadcast and Multicast Security	Chapter 12 in CG12 and Notes	Week 6 - Lecture 6 (2/3)
7. Trusted Platform	Sec. 12.3-12.4 in Chapter 13 in CG12 and Notes, and Sec. 3.3.2 and Sec. 9.1, 9.6-9.7 in GT11 and notes.	Lecture 6 (1/3), Week 7 - Lecture 7
8. Decentralized System Security	Notes and some selected research articles, which will be provided.	Weeks 8-9, Lectures 8-9
9. Privacy Enhanced Technologies	Notes and some selected research articles, which will be provided.	Week 10, Lecture 10
10. Post-quantum and Quantum Cryptography	Notes.	Week 11, Lecture 11
Project Presentation		Week 12

* NIST, Standards for Security Categorization of Federal Information and Information Systems, FIPTS-PUB-199, `http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf`.

Course Grading

The overall grade is based on a midterm exam (take-home exam), one project (individual or 2-person group) and one final exam (open book exam, but only lecture slides are allowed to bring). For the project, a list of the project problems will be provided. A 5-8 minutes presentation slides and a report of 5-10 pages in an academic research article format are a must to obtain the score for the project. The due dates (all will be 11:59am ET) and the distribution of the marks are given

below. The answers of the midterm exam and the slides and report of the project will be submitted to Dropbox on Learn.

Note. For each topic, there are assignment questions for helping you to understand the course materials and to prepare for the exams.

Other Resources

- Matthew Green on cryptography engineering, `https://blog.cryptographyengineering.com/useful-cryptography-resources/`
- Schneier on Security, http://www.schneier.com/blog/. A blog covering current computer security and privacy issues.

Academic Integrity, Discipline, Grievances, and Appeals

Academic Integrity: In order to maintain a culture of academic integrity, members of the University of Waterloo community are expected to promote honesty, trust, fairness, respect and responsibility. [Check `www.uwaterloo.ca/academicintegrity/` for more information.]

Grievance: A student who believes that a decision affecting some aspect of his/her university life has been unfair or unreasonable may have grounds for initiating a grievance. Read Policy 70, Student Petitions and Grievances, Section 4, `www.adm.uwaterloo.ca/infosec/Policies/policy70.htm`. When in doubt please be certain to contact the departments administrative assistant who will provide further assistance.

Discipline: A student is expected to know what constitutes academic integrity [check `www.uwaterloo.ca/academicintegrity/`] to avoid committing an academic offence, and to take responsibility for his/her actions. A student who is unsure whether an action constitutes an offence, or who needs help in learning how to avoid offences (e.g., plagiarism, cheating) or about rules for group work/collaboration should seek guidance from the course instructor, academic advisor, or the undergraduate Associate Dean. For information on categories of offences and types of penalties, students should refer to Policy 71, Student Discipline, `www.adm.uwaterloo.ca/infosec/Policies/policy71.htm`. For typical penalties check Guidelines for the Assessment of Penalties, `www.adm.uwaterloo.ca/infosec/guidelines/penaltyguidelines.htm`.

Appeals: A decision made or penalty imposed under Policy 70 (Student Petitions and Grievances) (other than a petition) or Policy 71 (Student Discipline) may be appealed if there is a ground. A student who believes he/she has a ground for an appeal should refer to Policy 72 (Student Appeals) `www.adm.uwaterloo.ca/infosec/Policies/policy72.htm`.

Note for Students with Disabilities: The Office for Persons with Disabilities (OPD), located in Needles Hall, Room 1132, collaborates with all academic departments to arrange appropriate accommodations for students with disabilities without compromising the academic integrity of the curriculum. If you require academic accommodations to lessen the impact of your disability, please register with the OPD at the beginning of each academic term [check `http://www.studentservices.uwaterloo.ca/disabilities/`].

Turnitin.com: Text matching software (Turnitin®) may be used to screen assignments in this course. Turnitin® is used to verify that all materials and sources in assignments are documented. Students' submissions are stored on a U.S. server, therefore students must be given an alternative (e.g., scaffolded assignment or annotated bibliography), if they are concerned about their privacy and/or security. Students will be given due notice, in the first week of the term and/or at the time assignment details are provided, about arrangements and alternatives for the use of Turnitin in this course.